## REMARKS

In the Office Action dated January 29, 2007, pending Claims 1-50 were examined. Claims 1-5, 7, 9-12, 14, 15, 17-31, 36-37, 49 and 50 were rejection. Claims 6, 8, 13, 16, 32-35 and 48 are objected to as being dependent upon a rejected base claim. In response, no claims are amended, no claims are cancelled and no claims are added. Applicants respectfully request reconsideration of pending Claims 1-50 in view of at least the following remarks.

### I. Claims Rejected Under 35 U.S.C. §102(b)

The Examiner has rejected Claims 1-5, 7, 9-12, 14 and 15 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 6,333,983 issued to Enichen et al. ("Enichen".) Applicants respectfully traverse this rejection.

Claim 1, as amended, recites the following claim features which are neither expressly nor inherently disclosed by Enichen:

> receiving a decoded scrambling key having a key size according to a first cryptographic protocol;
>
> reducing the key size of the decoded scrambling key to match a key size of a second cryptographic protocol to form a reduced key size descrambling key whose value is a function of every bit of the decoded scrambling key; and
>
> descrambling received scrambled content according to the reduced key size descrambling key.

Enichen is generally directed to a method and apparatus for performing 56-bit DES encryption of data for financial processing or other purposes using a cryptographic facility whose data encryption and decryption functions have been degraded to conform with export limitations. In contrast with Claim 1, Enichen does not disclose or suggest reducing the key size of the decoded scrambling key to match a key size of a second cryptographic protocol, much less a reduced key size descrambling key whose value is a function of every bit of the decoded scrambling key, as in Claim 1. Enichen does disclose a transformation function for transforming a block, encrypted under a first key, to the same block encrypted under a second key (see Abstract), however, that is something completely different from reducing the key size of the decoded scrambling key to match a key size of a second cryptographic protocol, as recited in Claim 1.

According to the Examiner, the above recited features of Claim 1 are disclosed by Enichen as follows:

> figures 5-19 and accompanying descriptions, whereas the use of weak/strong derived keys and associated transport, KEK, etc., in the at least DES cryptographic environment (i.e., first/second cryptographic protocols; single or multiple encrypted/decrypted) insofar as the said keys are size adjusted (i.e., single/double length) dependent on the cryptographic primitives used, clearly encompasses the claim limitations, as broadly interpreted by the examiner. (p. 3, ¶ 1 of the Office Action mailed January 29, 2007.) (Emphasis added.)

Applicant first respectfully submits that the above characterization of Enichen is directed to a transformation function for transforming a block, encrypted under a first key, to the same block encrypted under a second key (See Abstract.) Neither this section nor any other disclosure in Enichen teaches or suggests reducing the key size of a decoded scrambling key to match a key size of a second cryptographic protocol, much less a reduced key size descrambling key whose value is a function of every bit of the decoded scrambling key, as in Claim 1.

Further, neither this section nor any other disclosure in Enichen teaches or suggests descrambling received scrambled content according to the reduced key size descrambling key per Claim 1. Apposite to Claim 1, Enichen discloses processing DES-encrypted data using increased size exporter and importer keys to decode scrambled content, as shown in FIG. 11. In fact, Enichen discloses a transformation function for transforming a block, encrypted under a first key, to the same block encrypted under a second key that enables emulation of a decryption function for descrambling of received content using repeated encryption (See FIG. 12.) Enichen teaches emulation of a decryption function which does not disclose or suggest descrambling received scrambled content according to the reduced key size descrambling key, as in Claim 1.

For each of the above reasons, therefore, Claim 1 and all claims which depend on it are patentable over the cited art.

Each of Applicants' other independent claims includes limitations similar to those in Claim 1 discussed above. Consequently, all of Applicant's other independent claims, and all claims which depend on them, are also patentable over the cited art, for similar reasons.

Therefore, Applicants respectfully request that the Examiner reconsider and withdraw the §102(b) rejection of Claims 1-5, 7, 9-12, 14 and 15, for at least the reasons described above.

The Examiner has rejected Claims 17-31 and 36-40 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 6,307,936 issued to Ober et al. ("Ober".) Applicants respectfully traverse this rejection.

Claim 17, as amended, recites the following claim features which are neither expressly nor inherently disclosed by Ober:

> a first cryptographic block that may be iterated without limit to descramble received information using one of an internal key and a preprogrammed key to form one of a descrambled key and descrambled data;
>
> a key feedback path to store the descrambled key as an internal key and to provide the one of the internal key and the preprogrammed key to a key input of the first cryptographic block; and
>
> a second cryptographic block to descramble received scrambled digital content using a final descrambling key from the first cryptographic block to form descrambled digital content.

Ober is generally directed to a method of creating and manipulating encryption keys without risking the security of the key. In contrast with Claim 1, Ober does not disclose or suggest a first cryptographic block that may be iterated without limit to descramble received information, much less that one of an internal key and a programmed key are used to descramble received information to form one of a descrambled key and descrambled data, as in Claim 17. Ober does disclose the selection of a key from one of a symmetrical key type and an asymmetrical key type as well as a key bit length followed by key generation and representation in external or internal form (see Abstract), however, that is something completely different from a key feedback path to store the descrambled key as an internal key and to provide the one of the internal key and the preprogrammed key to a key input of the first cryptographic block, as recited in Claim 17.

Furthermore, Ober does not disclose or suggest a second cryptographic block to descramble received digital content using a final descrambling key from a first cryptographic block to form descrambled digital content, as in Claim 17. According to the Examiner, the above recited features of Claim 17 are disclosed by Ober as follows:

> figures 1-4 and accompanying descriptions, and section III, whereas the management/creation of keys in a cryptographic co-processor insofar as the key management/creation allows for 'highly layered and complex ... key management (i.e., col. 1, lines 58-col. 2, line 14)' and associated storage/access configurability internally or externally, clearly encompasses the claim limitations, as broadly interpreted by the examiner. (See page 11, ¶ 1 of the Office Action mailed 01/29/07.)

We submit that the above characterization of Ober is directed to the managing of the use of keys in a cryptographic co-processor which includes the steps of key type selection, key length selection and representation of the generated key in either external form or internal form (see col. 1, lines 61-67.) Neither this section nor any other disclosure in Ober teaches or suggests a key feedback path to store a descrambled key received from a first cryptographic block as an internal key and providing either the descrambled key or a preprogrammed key to a key input of the first cryptographic block, much less a second cryptographic block that descrambles received scrambled digital content using a final descrambling key received from the first cryptographic block to form descrambled digital content, as in Claim 17.

Further, neither the above section nor any other disclosure in Ober teaches or suggests a first cryptographic block that may be iterated without limit to descramble received information, much less that such descrambling is performed using one of an internal key and a programmed key to form one of a descrablmed key and descrambled data, as in Claim 17.

For each of the above reasons, therefore, Claim 17 and all claims which depend on it are patentable over the cited art.

Each of Applicants' other independent claims includes limitations similar to those in Claim 17 discussed above. Consequently, all of Applicant's other independent claims, and all claims which depend on them, are also patentable over the cited art, for similar reasons. Therefore, Applicants respectfully request that the Examiner reconsider and withdraw the §102(b) rejection of Claims 17-31 and 36-40, for at least the reasons described above.

## II. Claims Rejected Under 35 U.S.C. §103

The Examiner has rejected Claims 41-47, 49 and 50 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,825,879 issued to Davis ("Davis") in view of Ober. Applicants respectfully traverse this rejection.

Regarding Claim 41, Claim 41 recites the following claims features which are neither expressly nor inherently disclosed by the prior art combination of Davis in view of Ober:

> a tuner to receive scrambled content;
>
> a CPU; and
>
> an integrated circuit select at least one of a preprogrammed key, internal key, external data and internal data under control of the CPU, comprising:
>
> a first cryptographic block to descramble received information using one of an internal key and a preprogrammed key to form one of a descrambled key and descrambled data,
>
> a key feedback path to iteratively store the descrambled information as one of an internal key and internal data, and to provide the one of the internal key and the preprogrammed key to a key input of the first cryptographic block and to provide the one of external data and the internal data to a data input of the first cryptographic block,
>
> a second cryptographic block to descramble received scrambled digital content using a final descrambling key from the first cryptographic block to form descrambled digital content, and
>
> a decoder to decode the descrambled digital content to form clear digital content.

We submit that Claim 41 recites analogous claim features to the previously described features of Claim 17. Therefore, Applicants' arguments provided above with regard to the anticipation rejection of Claim 17 equally apply to the Examiner's citing of Ober and the combination of Davis in view of Ober to render Claim 41 obvious.

For each of the above reasons, the key management scheme taught by Ober fails to teach or suggest at least the first cryptographic block, the key feedback path or the second cryptographic block which are used to form descrambled digital content. Furthermore, we submit that the Examiner's citing of Davis fails to rectify the deficiencies of Ober to teach the above recited features of Claim 41. Hence, the prior art combination of Davis in view of Ober fails to teach or suggest each of the above recited features of Claim 41.

For each of the above reasons, therefore, Applicant respectfully submits that Claim 41 and all claims which depend on it are patentable over the cited art. Therefore, Applicant respectfully requests that the Examiner reconsider and withdraw the §103(a) rejection of Claims 41-47, 49 and 50.

DEPENDENT CLAIMS

In view of the above remarks, a specific discussion of the dependent claims is considered to be unnecessary. Therefore, Applicants' silence regarding any dependent claim is not to be interpreted as an agreement with, or acquiescence to, the rejection of such claim or as waiving any argument regarding that claim.

## III. Allowable Subject Matter

The Examiner has objected to Claims 6, 8, 13, 16, 32-35 and 48 as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form, including all of the limitations of the base claim and any intervening claims.

Applicants respectfully thank the Examiner for recognizing the allowability of Claims 6, 8, 13, 16, 32-35 and 48. However, for at least the reasons provided above, Applicants respectfully submit that such claims, based on their dependency from independent Claims 1, 9, 17 and 41, are also patentable over Davis in view of Ober, as well as the references of record. Therefore, Applicants respectfully request that the Examiner reconsider and withdraw the objection to Claims 6, 8, 13, 16, 32-35 and 48, and allow such claims, based on their dependencies from Claims 1, 9, 17 and 41.

## CONCLUSION

In view of the foregoing, it is believed that all claims now pending (1) are in proper form, (2) are neither obvious nor anticipated by the relied upon art of record, and (3) are in condition for allowance. A Notice of Allowance is earnestly solicited at the earliest possible date. If the Examiner believes that a telephone conference would be useful in moving the application forward to allowance, the Examiner is encouraged to contact the undersigned at (310) 207-3800.

If necessary, the Commissioner is hereby authorized in this, concurrent and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17, particularly, extension of time fees.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Dated: 4/24/07 By: ______________________

Joseph Lutz, Reg. No. 43,765

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
Telephone (310) 207-3800
Facsimile (310) 820-5988

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being submitted electronically via EFS Web on the date shown below to the United States Patent and Trademark Office.

Suzanne Johnston 4/24/07
Date